

IN THE CLAIMS:

The following listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for providing secure network communication, comprising:

providing an intelligent network interface between a network and each node on the network;

encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces; and

centrally managing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network with a central management console (CMC).

2. (Previously Presented) The method of claim 1, further comprising each intelligent network interface providing protocol translation based on servlets provided by said CMC.

3. (Previously Presented) The method of claim 2, wherein said protocol translation is selected from the any two protocols within a single layer of an ISO 7 layer protocol stack.

4. (Previously Presented) The method of claim 2, further comprising said CMC dynamically distributing proxy servlets to intelligent network interfaces based on distinguished name.

5. (Previously Presented) The method of claim 2, further comprising said CMC dynamically distributing servlets to intelligent network interfaces based on distinguished name, said servlets selected from the group consisting of single sign-on servlets, distinguished name firewall servlets, auditing servlets, policy enforcement servlets, and web-filtering servlets.

6. (Previously Presented) The method of claim 2, further comprising said CMC dynamically distributing servlets to intelligent network interfaces based on node, said servlets selected from the group consisting of fault tolerance automatic rollover servlets, gateway intrusion detection servlets, multi-level firewall servlets, machine diagnostics servlets, virus scanning servlets, and security patching servlets.

7. (Previously Presented) The method of claim 1, further comprising:

a first intelligent network interface associated with a first client sending a request to the central management console (CMC) with the identifying information about a

connection that the first client wishes to send to a second client, said information including protocol, distinguished name, service, and header information;

said CMC reviewing said connection against a network policy and determining denial or allowance of said connection and, upon allowance, further determining encryption algorithm, authentication required, keys for the connection, if the connection should be redirected to another node, and if the connection needs to be translated;

said CMC sending a connection determination, including encryption and authentication algorithm(s), key(s), and any translation servlets required to said first intelligent network interface;

said first intelligent network interface initiating said connection with a second intelligent network interface associated with said second client by sending encrypted connection information with authentication;

said second intelligent network interface querying said CMC with said encrypted connection information received from said first intelligent network interface, including a Security Parameters Index (SPI) for said connection that uniquely identifies said connection between said first and second intelligent network interfaces.

8. (Previously Presented) The method of claim 7, wherein said

authentication is selected from the group consisting of username/password, biometric inputs, smart cards, tokens, and combinations thereof.

9. (Previously Presented) The method of claim 1, further comprising providing a plurality of CMCs on said network in a hierarchical configuration.

10. (Previously Presented) A method for providing distinguished name single sign-on for users of host devices on a network comprising:

- providing an intelligent network interface between a network and each device on the network;

- providing a central management console (CMC) on said network;

- a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device;

- the first intelligent network interface verifying the user's authentication with the CMC such that when said user requests services from a second device:

- the first intelligent network interface requests communication with said second device based on distinguished name;

- a second intelligent network interface associated

with said second device queries the CMC for permission and user authentication for the second device based on distinguished name; and

the CMC provides user authentication information based on distinguished name to said second intelligent network interface to allow said second intelligent network interface to log the user into the second device.

11. (Previously Presented) A system for providing secure network communication, comprising:

a network;

a plurality of host devices connected to said network;

an intelligent network interface between each host device and said network;

means on each intelligent network interface for encrypting and decrypting critical data transmissions over the network; and

at least one central management console for providing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network.

12. (Previously Presented) The system of claim 11, wherein each intelligent network interface further comprises:

a CPU;
memory;
an I/O interface for the network; and
a second I/O interface for the host device.

13. (Previously Presented) The system of claim 12, wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI cards, PCMCIA cards, rapid I/O-high bandwidth cards, and standalone devices.

14. (Previously Presented) The system of claim 12, wherein each intelligent network interface is implemented in a form selected from the group consisting of PCI NIC cards, PCMCIA NIC cards, rapid I/O-high bandwidth NIC cards, and standalone devices with an Ethernet second I/O interface.

15. (Previously Presented) The system of claim 12, wherein each intelligent network interface further comprises a serial line authentication port.

16. (Previously Presented) The system of claim 15, wherein said serial line authentication port is a USB port.

17. (Previously Presented) The system of claim 12, wherein said intelligent network interface further comprises parallel port

authentication port.

18. (Previously Presented) The system of claim 12, wherein said memory consists of flash memory for storing an Operating System (OS) and dynamic memory for applications.

19. (Previously Presented) The system of claim 12, wherein said memory consists of a hard drive for storing an Operating System (OS) and applications and random access memory for running said OS and applications.

20. (Previously Presented) The system of claim 12, wherein said intelligent network interfaces have an Operating System (OS) that is distinct from said host device's OS.

21. (Previously Presented) The system of claim 12, further comprising:

an encryption accelerator on a field programmable gate array (FPGA) on said intelligent network interface.

22. (Previously Presented) The system of claim 11, further comprising:

a set of dynamically distributable code fragments stored on said CMC for distribution to said intelligent network interfaces; and

means on each said intelligent network interface for using said code fragments to provide functions selected from the group consisting of: authentication, protocol translations, single sign-on, multi-level firewalling, distinguished-name based firewalling, centralized user management, machine diagnostics, proxying, fault tolerance, centralized patching, web filtering, virus scanning, auditing, and gateway intrusion detection.

Claims 23-34 (Canceled)

35. (Previously Presented) A method for firewalling based on distinguished name for users of host devices on a network comprising:

- providing an intelligent network interface between a network and each device on the network;
- providing a central management console (CMC) on said network;
- a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device;
- the first intelligent network interface verifying the user's authentication with the CMC; and
- the CMC dynamically distributing a firewall servlet to said intelligent network interface based on said distinguished

AMENDMENT UNDER 37 C.F.R. § 1.111
Appln. No. 10/068,776

PATENT APPLICATION

name.

Claim 36 (Canceled)